



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,629	08/16/2001	Steven Dale Goodman	RPS9 2001 0046	2708

45211 7590 10/14/2004

KELLY K. KORDZIK  
WINSTEAD SECHREST & MINICK PC  
PO BOX 50784  
DALLAS, TX 75201

EXAMINER

CHAI, LONGBIT

ART UNIT PAPER NUMBER

2131

DATE MAILED: 10/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/931,629

Applicant(s)

GOODMAN ET AL.

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 09 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☐ Claim(s) \_\_\_\_\_ is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 16 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## DETAILED ACTION

### *Priority*

1. No claim for priority has been made in this application.
2. The effective filing date for the subject matter defined in the pending claims in this application is 8/16/2001.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 4, 7, 8 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (Patent Number: US 6363463 B1), hereinafter referred to as Mattison, in view of Grawrock ("Building Trusted and Privacy into Open PC Systems", Nov. 2000), hereinafter referred to as Grawrock.
4. As per claim 1, 4, 7, 8 and 10, Mattison teaches a computer program product adaptable for storage on a computer readable medium and operable for updating a BIOS stored in a flash memory in a data processing system, comprising:

Art Unit: 2131

5. a BIOS update application program receiving an updated BIOS image; the original target BIOS program performing the signature verification of the updated BIOS image and posting a result of the signature verification of the updated BIOS image to the BIOS update application (Mattison: see for example, Column 3 Line 23 – 62).
6. Mattison does not teach expressly teach a specific TPM (Trusted Platform Module).
7. Grawrock teaches a TPM is defined by TPCA (Trusted Platform Computing Alliance) and performs the authorization, correct use and proper measurement for the BIOS boot loader through the digital signature technique (Grawrock, see example, Page 4 Definitions section, Authenticated Boot section and Summary section 2<sup>nd</sup> Paragraph Line 4).
8. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Grawrock within the system of Mattison because Grawrock teaches a method of trusted computing platform to enhance the security and protecting privacy, especially for the BIOS boot process (Grawrock: see for example, section of Overview 2<sup>nd</sup> Paragraph Line 5 and section of Authenticated Boot 1<sup>st</sup> Paragraph Line 2 – 3).
9. Therefore, Mattison as modified teaches:
10. the BIOS update application requesting a TPM to perform a signature verification of the updated BIOS image; a TPM program receiving the request from the BIOS update application to perform the signature verification of the updated BIOS image; and the TPM program performing the signature verification of the updated BIOS image and

Art Unit: 2131

posting a result of the signature verification of the updated BIOS image to the BIOS update application (Mattison: see for example, Column 3 Line 23 – 62) & (Grawrock, see example, Page 4 Definitions section and Authenticated Boot section).

11. As per claim 7 and 10, Mattison as modified teaches the claimed invention as described above (see claim 6 and 8 respectively). Mattison as modified further teaches if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is not authentic, then an error message is output (Grawrock: see for example, section of Authenticated Boot, 1<sup>st</sup> Paragraph, Line 2 and Line 6).

12. Claims 2, 3, 5, 6 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mattison (Patent Number: US 6363463 B1), hereinafter referred to as Mattison, in view of Grawrock ("Building Trusted and Privacy into Open PC Systems", Nov. 2000), hereinafter referred to as Grawrock, and in view of Hale (Patent Number: US 6564371 B1), hereinafter referred to as Hale.

13. As per claim 2 and 9, Mattison as modified teaches the claimed invention as described above (see claim 1 and 8 respectively). Mattison as modified does not teach expressly locking the memory unit after the modifying step.

14. Hale teaches locking the memory unit after the modifying step (Hale: see for example, Column 11 Line 21 – 23 and Column 8 Line 1 – 2).

Art Unit: 2131

15. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hale within the system of Mattison as modified because (a) Grawrock teaches the TPM needs to assure the correct use of the authorization process (Grawrock: see for example, section of Definitions 1<sup>st</sup> Bullet Line 2) (b) Hale teaches a method of correct use of nonvolatile memory update through a locking mechanism (Hale: see for example, Column 3 Line 50 – 54).

16. As per claim 3, Mattison as modified teaches the claimed invention as described above (see claim 2). Mattison as modified further teaches the locking step is performed by the TPM (Grawrock: see for example, section of Definitions 1<sup>st</sup> Bullet Line 2).

17. As per claim 5, Mattison as modified teaches the claimed invention as described above (see claim 4). Mattison as modified teaches that TPM performs the signature verification of the updated BIOS image and determines that the updated BIOS image is authentic (Mattison: see for example, Column 3 Line 23 – 62) & (Grawrock, see example, Page 4 Definitions section and Authenticated Boot section).

18. Mattison as modified does not teach expressly if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory.

19. Hale teaches if the result of the signature verification of the updated BIOS image determines that the updated BIOS image is authentic, then the TPM program unlocks the flash memory (Hale: see for example, Column 11 Line 21 – 23 and Column 3 Line 50 – 54: Hale teaches unlocking the memory if the nonvolatile memory update is ready to process).

Art Unit: 2131

20. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Hale within the system of Mattison as modified because (a) Grawrock teaches the TPM needs to assure the correct use of the authorization process (Grawrock: see for example, section of Definitions 1<sup>st</sup> Bullet Line 2) (b) Hale teaches a method of correct use of nonvolatile memory update through a locking mechanism (Hale: see for example, Column 3 Line 50 – 54).

21. Mattison as modified further teaches the BIOS update application modifies the BIOS with the updated BIOS image (Mattison: see for example, Column 3 Line 60 – 62).

22. As per claim 6, Mattison as modified teaches the claimed invention as described above (see claim 5). Mattison as modified further teaches programming for locking the flash memory after the BIOS update application modifies the BIOS with the updated BIOS image (Hale: see for example, Column 11 Line 21 – 23).

Art Unit: 2131

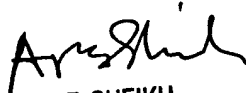
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai  
Examiner  
Art Unit 2131

LBC

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100